BRIAN J. STRETCH (CABN 163973)
United States Attorney

DAVID R. CALLAWAY (CABN 121782)
Chief, Criminal Division

HELEN L. GILBERT (NYBN 4736336)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7021
FAX: (415) 436-7234
Helen.Gilbert@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. BRYAN GILBERT HENDERSON, Defendant.	No. CR 15-0565 WHO UNITED STATES' RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS NIT SEARCH WARRANT ~~UNDER SEAL~~ Hearing date: August 18, 2016 Hearing time: 1:30 p.m.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

I. INTRODUCTION

Playpen was a website dedicated to sharing child pornography that operated on the anonymous Tor network. After a months-long investigation, the FBI apprehended the administrator of Playpen and seized the website from the web-hosting facility where it had been run. Because the site operated on the Tor network, law enforcement officials were unable to determine the actual identities and location of Playpen's users without employing additional investigative techniques. Therefore, the FBI briefly assumed administrative control of Playpen and allowed the website to continue to operate at a government facility in the Eastern District of Virginia. At the same time, the FBI sought and obtained a warrant from a magistrate judge in the Eastern District of Virginia permitting it to deploy a Network Investigative Technique ("NIT") that would cause a computer logging into Playpen to reveal certain specific information that would help law enforcement officials locate and identify Playpen users.

Using the NIT, the FBI procured the IP address associated with Playpen user "askjeff." After conducting further investigation, the FBI determined that this IP address resolved to the defendant, Bryan Henderson. The FBI procured a search warrant from a magistrate judge in the Northern District of California to search Henderson's home in San Mateo, California. The search warrant was executed and after finding child pornography on the defendant's computer, he was arrested and charged by superseding indictment with receipt and possession of child pornography.

The defendant now brings a narrow challenge to the warrant: he does not claim that the warrant lacked probable cause and does not meaningfully contest that the warrant met the Fourth Amendment's particularly requirements. Instead, the defendant argues that the NIT warrant did not comply with Federal Rule of Criminal Procedure 41(b) and 28 U.S.C. § 636(a) because the magistrate judge could only issue a warrant for a location within the Eastern District of Virginia. Because of this purported violation, the defendant argues for suppression of all evidence obtained based on the NIT warrant.

The NIT warrant was entirely consistent with the Fourth Amendment, Federal Rule of Criminal Procedure 41, and the Federal Magistrates Act, 28 U.S.C. § 636(a). As the Supreme Court and the Ninth Circuit have explained, Rule 41 should be construed broadly so as to uphold otherwise constitutionally valid search warrants where possible. The FBI sought a warrant to deploy the NIT in the district with the greatest connection to the activity, that is, the district where Playpen was operating. In a 31-page

affidavit, the FBI presented a fulsome explanation of Playpen, the Tor network, how the NIT would operate, and the limited information (and the purpose for procuring that information) that would be returned from users' computers. Even if the NIT warrant was somehow lacking, the extraordinary remedy of suppression is inappropriate here, where the Eastern District of Virginia magistrate judge had the authority to issue the warrant, any such violation was merely technical, not constitutional, the defendant was not prejudiced, and the government acted in good faith and without intentional and deliberate disregard of the law. Furthermore, even if the warrant were unauthorized, the use of the NIT would still have been justified by exigent circumstances.

The defendant essentially argues that no magistrate judge could have issued the NIT warrant. Under the defendant's interpretation of Rule 41(b), individuals who hide their location through anonymizing technologies in order to avoid detection while conducting criminal activity can claim that because their location was unknown, no magistrate judge has the authority to issue a warrant supported by probable cause to determine that individual's location. This absurd and circular result is inconsistent with the letter and spirit of Rule 41(b) and inconsistent with the Fourth Amendment. The defendant's motion to suppress should be denied.

II. BACKGROUND

The charges in this case arise from an investigation into Playpen, referred to in two search warrants at issue here as "Website A,"[1] a global online forum through which registered users (including the defendant) advertised, distributed, and/or accessed illegal child pornography. The scale of child sexual exploitation on the site was massive: more than 150,000 total members created and viewed tens of thousands of postings related to child pornography. Images and videos shared through the site were highly categorized according to victim age and gender, as well as type of sexual activity. The site also included forums for the discussion of all things related to child sexual exploitation, including tips for grooming victims and avoiding detection.

[1] Law enforcement officials did not disclose the name of the website, Playpen, or the network on which it operated, the Tor network, in the search warrants at issue here due to concern that their disclosure would alert targets of the on-going investigation. The name of the website and network have since been identified publicly, and are referred to throughout this brief by their proper names.

A. Playpen users, including Henderson, used the Tor network to access child pornography while avoiding law enforcement detection.

Playpen operated on the anonymous Tor network. Tor, which standards for the onion router, was created by the U.S. Naval Research Laboratory as a means of protecting government communications. It is now available to the public. Use of the Tor network masks a user's actual Internet Protocol ("IP") address, which could otherwise be used to identify a user, by bouncing user communications around a network of relay computers (called "nodes") run by volunteers.[2] To access the Tor network, a user must install Tor software either by downloading an add-on to their web browser or the free "Tor browser bundle." Users can also access Tor through "gateways" on the open Internet that do not provide users with the full anonymizing benefits of Tor. When a Tor user visits a website, the IP address visible to that site is that of a Tor "exit node," not the user's actual IP address. Tor is designed to prevent tracing the user's actual IP address back through that Tor exit node. Accordingly, traditional IP-address-based identification techniques used by law enforcement on the open Internet are not viable on the Tor network.

Within the Tor network itself, certain websites, including Playpen, operate as "hidden services." Like other websites, they are hosted on computer servers that communicate through IP addresses. They operate in the same way as other public websites with one critical exception: the IP address for the web server is hidden and replaced with a Tor-based web address, which is a series of sixteen algorithm-generated characters followed by the suffix ".onion." A user can only reach a "hidden service" by using the Tor client and operating in the Tor network. And unlike an open Internet website, it is not possible to use public lookups, such as search engines, to determine the IP address of a computer hosting a "hidden service."

A "hidden service," like Playpen, is also more difficult for users to find. Even after connecting to the Tor network, users must know the exact web address of a "hidden service" in order to access it. Accordingly, in order to find Playpen, a user had to first get the web address for it from another source—such as another Playpen user or online postings identifying Playpen's content and

[2] Additional information about Tor and how it works can be found at www.torproject.org.

location. Accessing Playpen thus required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon it without first understanding its child pornography-related content and purpose.

Although the FBI was able to view and document the substantial illicit activity occurring on Playpen, investigators faced a tremendous challenge when it came to identifying Playpen users. Because Tor conceals IP addresses, normal law enforcement tools for identifying Internet users would not work. So even if law enforcement managed to locate Playpen and its IP logs, traditional methods of identifying users would have been unsuccessful.

Acting on a tip from a foreign law enforcement agency, as well as information from its own ongoing investigation, the FBI determined that the computer server that hosted Playpen was located at a web-hosting facility in North Carolina. In February 2015, FBI agents apprehended the administrator of Playpen and seized the website from its web-hosting facility. Rather than immediately shut the site down, which would have allowed the users of Playpen to go unidentified (and un-apprehended), the FBI allowed Playpen to continue to operate at a government facility in the Eastern District of Virginia for the brief period from February 20, 2015 through March 4, 2015, in order to gather information about Playpen's users.

On February 20, 2015, the FBI obtained a warrant from a magistrate judge of the United States District Court for the Eastern District of Virginia to deploy a Network Investigative Technique ("NIT") on the site (hereinafter, "NIT warrant"), in order to attempt to locate and identify registered users who were anonymously engaging in the sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation.[3]

Using the NIT, the FBI identified an IP address, a computer host name, "KALUMAN-PC," and a computer logon name, "kaluman," all associated with Playpen user "askjeff." The FBI traced this IP address, computer host name, and computer logon name to Bryan Henderson. The IP address

[3] Unsealed, redacted versions of the NIT search warrant, application, affidavit, and return (No. 15-SW-89) are attached as Government Exhibit A. Law enforcement officials also sought and obtained a Title III order on February 20, 2015, from the U.S. District Court for the Eastern District of Virginia to intercept electronic communication occurring over the private message and private chat functions of Playpen. This Title III order is not challenged here, but unsealed, redacted copies of the Title III order, application, and affidavit (No. 15-ES-4) are attached as Government Exhibit C.

was registered to Elizabeth Henderson, Bryan Henderson's then-99-year-old grandmother, at her home where Bryan Henderson and his brother Matthew Henderson live. On August 24, 2015, FBI Special Agent Kelli Johnson obtained a residential search warrant for Henderson's home in San Mateo, California, from United States Magistrate Judge Joseph C. Spero (hereinafter, "San Mateo warrant").[4] Agents executed the warrant at Henderson's home on September 2, 2015, and seized over forty digital devices. Elizabeth Henderson and Bryan Henderson were both present at the home during the execution of the search warrant. After being advised that he was not under arrest and was free to leave at any time, Bryan Henderson agreed to be interviewed. Henderson stated that he used the Tor network and that "kaluman" was the name of his computer, which was found in Henderson's bedroom. Henderson denied visiting Playpen and denied viewing child pornography.

The initial forensic review confirmed the presence of images of child pornography on Henderson's computer. On November 3, 2015, Henderson was arrested for possession of child pornography. After being advised of his rights, Henderson agreed to be interviewed. He again stated that the "kaluman" computer was his and that he used the Tor network. Henderson was indicted on one count of possession of child pornography. *See* Dkt. 13. The grand jury later issued a superseding indictment, charging Henderson with possession and receipt of child pornography. *See* Dkt. 26.

B. The nature of Playpen and the Tor network required law enforcement to seek court approval to deploy a NIT to identify criminals engaged in the creation, advertisement, and distribution of child pornography.

1. The NIT warrant set forth in great detail the technical aspects of the investigation that justified law enforcement's request to use the NIT.

The 31-page NIT warrant affidavit was sworn by a veteran FBI agent with 19 years of federal law enforcement experience and particular training and experience investigating child pornography and the sexual exploitation of children. Gov. Ex. A, at 5, ¶ 1. In recognition of the technical and legal complexity of the investigation, the NIT search warrant affidavit included: a three-page explanation of the offenses under investigation, Gov. Ex. A, at 6-8, ¶ 4; a seven-page section setting out definitions of technical terms used in the affidavit, *id.* at 8-14, ¶ 5; and a three-page explanation of

[4] The San Mateo search warrant, application, affidavit, and return, *In the Matter of the Search of 1106 E. 16th Avenue, San Mateo, California 94402*, are attached as Government Exhibit B.

the Tor network, how it works, and how users could find a hidden service such as Playpen, *id.*, at 14-17, ¶¶ 7-10. The affidavit spelled out the numerous affirmative steps a user would have to go through just to find the site:

> Even after connecting to the Tor network, however, a user must know the web address of the website in order to access the site. Moreover, Tor hidden services are not indexed like websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography. [Playpen] is listed in that section.

Id., at 16-17, ¶ 10. Thus, the agent continued, "[a]ccessing [Playpen] . . . requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon [it] without understanding its purpose and content." *Ibid.*

2. Playpen was dedicated to the advertisement and distribution of child pornography, a fact that would have been apparent to anyone who viewed the site.

The affidavit also described in great detail the purpose of Playpen and why its users were appropriate targets for the NIT. Playpen was "dedicated to the advertisement and distribution of child pornography," "discussion of . . . methods and tactics offenders use to abuse children," and "methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes." *Id.* at 14, ¶ 6. More to the point, "administrators and users of [Playpen] regularly sen[t] and receive[d] illegal child pornography via the website." *Ibid.* The agent also explained the sheer scale of the illicit activity occurring on Playpen: site statistics as of February 3, 2015, for Playpen—which was believed to have been in existence only since August of 2014—showed that it contained 158,094 members, 9,333 message threads, and 95,148 posted messages.[5] *Id.*

[5] As the affidavit explained, a bulletin board website such as Playpen is a website that provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Gov. Ex. A, at 8, ¶5(a).

at 17, ¶ 11.

Playpen's illicit purpose was also apparent to anyone who visited it during the six months it operated before the FBI seized control of it. "[O]n the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart." *Id.* at 17, ¶ 12. And the following text appeared beneath those young girls: "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." *Ibid.* While those terms may have seemed insignificant to the untrained eye, the affiant explained, based on his training and his experience, that the phrase "no cross-board reposts" referred to a "prohibition against material that is posted on other websites from being "re-posted" to Playpen and that ".7z" referred to a "preferred method of compressing large files or sets of files for distribution." *Id.* at 17-18, ¶ 12. The combination of sexualized images of young girls along with these terms of art referencing image posting and large file compression unmistakably marked Playpen as just what it was—a hub for the trafficking of illicit child pornography.

The affidavit also explained that users were required to register an account by creating a username and password before they could access the site and highlighted the emphasis the registration terms placed on users avoiding identification. Users clicking on the "register an account" hyperlink on the main page were required to accept registration terms, the entire text of which was included in the affidavit. *Id.* at 18-19, ¶¶ 12-13. Playpen repeatedly warned prospective users to be vigilant about their security and the potential to be identified, explicitly stating, "the forum operators do NOT want you to enter a real [e-mail] address," users "should not post information [in their profile] that can be used to identify you," "it is impossible for the staff or the owners of this forum to confirm the true identity of users," "[t]his website is not able to see your IP," and "[f]or your own security when browsing or Tor we also recomend [sic] that you turn off javascript and disable sending of the 'referer' header." *Id.* at 18-19, ¶ 13. This focus on anonymity is entirely consistent with the desire on the part of Playpen administrators and users to evade detection of their illicit activities.

Once a user accepted those terms and conditions, a user was required to enter a username, password, and e-mail address. *Id.* at 19 ¶ 14. Upon successful registration, all of the sections, forums,

and sub-forums, along with the corresponding number of topics and posts in each, were observable. *Id.* at 19, ¶ 14. The vast majority of those sections and forums were categorized repositories for sexually explicit images of children, sub-divided by gender and the age of the victims. For instance, within the site's "Chan" forum were individual sub-forums for "jailbait" or "preteen" images of boys and girls. *Ibid.* There were separate forums for "Jailbait videos" and "Jailbait photos" featuring boys and girls. *Ibid.* The "Pre-teen Videos" and "Pre-teen Photos" forums were each divided into four sub-forums by gender and content, with "hardcore" and "softcore" images/videos separately categorized for Boys and Girls. *Id.* at 16, ¶ 14. A "Webcams" forum was divided into Girls and Boys sub-forums. *Ibid.* The "Potpurri" forum contained subforums for incest and "Toddlers." *Ibid.*

The affidavit also described, in graphic detail, particular child pornography that was available to all registered users of Playpen, including images of prepubescent children, and even toddlers, being sexually abused by adults. *Id.* at 21-22, ¶ 18. Although the affidavit clearly stated that "the entirety of [Playpen was] dedicated to child pornography," it also specified a litany of site sub-forums which contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children." *Id.* at 24-25, ¶ 27.

The affidavit further explained that Playpen contained a private messaging feature that allowed users to send messages directly to one another. The affidavit specified that "numerous" site posts referenced private messages related to child pornography and exploitation, including an example where one user wrote to another, "I can help if you are a teen boy and want to fuck your little sister, write me a private message." *Id.* at 22-23, ¶ 21. According to the affiant's training and experience and law enforcement's review of the site, the affiant stated his belief that the site's private message function was being used to "communicate regarding the dissemination of child pornography." *Id.* at 23, ¶ 22. The affidavit also noted that Playpen included multiple other features intended to facilitate the sharing of child pornography, including an image host, a file host, and a chat service. *Id.* at 23-24, ¶¶ 23-25. All of those features allowed site users to upload, disseminate, and access child pornography. And the affidavit included detailed examples and graphic descriptions of prepubescent child pornography disseminated by site users through each one of those features. *Ibid.*

3. The affidavit and attachments explained what the NIT would do and precisely identified the seven pieces of information it would collect and send back to government-controlled computers.

The affidavit contained a detailed and specific explanation of the NIT, its necessity, how and where it would be deployed, what information it would collect, and why that information constituted evidence of a crime.

Specifically, the affidavit noted that without the use of the NIT "the identities of the administrators and users of [Playpen] would remain unknown" because any IP address logs of user activity on Playpen would consist only of Tor "exit nodes," which "cannot be used to locate and identify the administrators and users." Gov. Ex. A, at 26, ¶ 29. Further, because of the "unique nature of the Tor network and the method by which the network . . . route[s] communications through multiple other computers, . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed." The affiant thus concluded, "using a NIT may help FBI agents locate the administrators and users" of Playpen. *Id.* at 27-28, ¶¶ 31-32. Indeed, he explained, based upon his training and experience and that of other officers and forensic professionals, that the NIT was a "presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove . . . the actual location and identity" of Playpen users who were "engaging in the federal offenses enumerated" in the warrant. *Id.* at 27, ¶ 31.

In terms of the deployment of the NIT, the affidavit explained that the NIT consisted of additional computer instructions that would be downloaded to a user's computer along with the other content of Playpen that would be downloaded through normal operation of the site. Gov. Ex. A, at 28, ¶ 33. Those instructions, which would be downloaded from the website located in the Eastern District of Virginia, would then cause a user's computer to transmit specified information to a government-controlled computer. *Ibid.* The discrete pieces of information to be collected were detailed in the warrant and accompanying Attachment A, along with technical explanations of the terms. They were limited to the following: (1) the actual IP address assigned to the user's computer; (2) a unique identifier to distinguish the data from that collected from other computers; (3) the operating system running on the computer; (4) information about whether the NIT had already been

delivered to the computer; (5) the computer's Host Name; (6) the computer's active operating system username; and (7) the computer's Media Access Control (MAC) address. *Id.* at 3, 28-29, ¶ 34.

The affidavit explained exactly why the information "may constitute evidence of the crimes under investigation, including information that may help to identify the . . . computer and its user." *Id.* at 30, ¶ 35. For instance:

> the actual IP address of a computer that accesses [Playpen] can be associated with an [Internet Service Provider ("ISP")] and a particular ISP customer. The unique identifier and information about whether the NIT has already been delivered to an "activating" computer will distinguish the data from that of other "activating" computers. The type of operating system running on the computer, the computer's Host Name, active operating system username, and the computer's MAC address can help to distinguish the user's computer from other computers located at a user's premises.

Ibid.

The affidavit requested authority to deploy the NIT each time any user logged into Playpen with a username and a password. *Id.* at 30, ¶ 36. And it also noted that the FBI might deploy the NIT more discretely against particular users, such as those who had attained a higher status on the site, "in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation." *Id.* at 28-29, ¶ 32, n. 8. Finally, the affidavit requested authority for the NIT to "cause an activating computer – wherever located – to send to a computer controlled by or known to the government . . . messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer." *Id.* at 33-34, ¶ 46(a).

III. ARGUMENT

The NIT warrant fully complied with the Fourth Amendment, with Federal Rule of Criminal Procedure 41, and with 28 U.S.C. § 636(a). Even assuming arguendo that the warrant was somehow lacking, the extraordinary remedy of suppression is inappropriate here, where the Eastern District of Virginia magistrate judge had the authority to issue the warrant, any such violation was merely technical, not constitutional, the defendant was not prejudiced, and the government acted in good faith and without intentional and deliberate disregard of the law. Furthermore, even if it were the case that no judge could have authorized the warrant, the use of the NIT would still have been justified by exigent circumstances.

Numerous motions to suppress the NIT warrant have been filed throughout the country, and to date, the government is aware of eight district courts that have issued opinions on this issue. Six courts have denied to suppress the NIT warrant. *See United States v. Matish*, No. 4:16-CR-16, Dkt. 90 (E.D. Va. Jun. 23, 2016); *United States v. Darby*, No. 2:16-CR-36, 2016 WL 3189703 (E.D. Va. Jun. 3, 2016); *United States v. Werdene*, No. 15-CR-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016); *United States v. Epich*, No.15-CR-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *United States v. Stamper*, No. 1:15CR109, 2016 WL 695660 (S.D. Ohio Feb. 19, 2016); *United States v. Michaud*, No. 3:14-CR-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). Two courts have suppressed the NIT warrant. *United States v. Arterbury*, No. 15-CR-182-JHP, Dkt. 47 (N.D. Okla. May 17, 2016); *United States v. Levin*, No. CR 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016). The defendant's arguments are without merit, and consistent with the majority of courts to have addressed this issue, his motion to suppress should be denied.

A. The NIT warrant fully complied with the Fourth Amendment, including the particularity requirement.

The NIT warrant fully complied with the Fourth Amendment: it was amply supported by probable cause, particularly described the place to be searched and items to be seized, and was issued by a neutral and detached magistrate. Furthermore, the use of the NIT was reasonable in light of the significant challenge of investigating Tor users who were hiding their identity and location while exploiting children online.

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const., Amend. IV. Henderson does not contest that the NIT warrant was supported by probable cause and was issued by a neutral and detached magistrate judge. The district courts that have addressed this issue have uniformly held that the NIT warrant was supported by probable cause. *See Darby*, 2016 WL 3189703, *8; *Matish*, Dkt. 90, *22; *Epich*, 2016 WL 953269, *1–2; *Michaud*, 2016 WL 337263, *16.

Henderson does argue that the NIT warrant failed to comply with the Fourth Amendment's particularly requirement. Def. Mot. to Suppress (hereinafter, "MTS"), at 16-17. The Fourth

Amendment's particularity requirement applies to "the place to be searched" and "the persons or things to be seized." *United States v. Grubbs*, 547 U.S. 90, 97 (2006). The place to be searched must be "described with sufficient particularity to enable the executing officer to locate and identify the premises with reasonable effort." *United States v. Turner*, 770 F.2d 1508, 1510 (9th Cir. 1985) (citations and quotations omitted). And the description of the items to be seized must not be "left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927). Whether this particularity standard is met is determined in light of the information available at the time the warrant issued. *United States v. Shi*, 525 F.3d 709, 731-32 (9th Cir. 2008).

The Fourth Amendment also places limits on the scope of a search. Specifically, "what may be seized" pursuant to a search warrant is "limited by the probable cause on which the warrant is based." *United States v. Brobst*, 558 F.3d 982, 993 (9th Cir. 2009). "[T]he scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe that it may be found.'" *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (quotations omitted). Therefore, "it is axiomatic that if a warrant sufficiently describes the premises to be searched, this will justify a search of the personal effects therein belonging to the person occupying the premises if those effects might contain the items described in the warrant." *United States v. Gomez-Soto*, 723 F.3d 649, 654 (9th Cir. 1984). For purposes of the Fourth Amendment, determining the proper scope of a search depends upon the relationship between the items to be seized under the warrant and the likelihood that they will be found in the places to be searched.

The NIT warrant meets both prongs of the Fourth Amendment's particularly requirement. The NIT warrant directs that the person or property to be searched is provided in Attachment A to the warrant. *See* Gov. Ex. A at 2. Attachment A, entitled the "Place to be Searched," defines the place to be searched with particularity. *See id.* at 3. It provides that the warrant authorizes "the use of the network investigative technique ("NIT") to be deployed on the computer server [that was hosting Playpen] . . . which will be located at a government facility in the Eastern District of Virginia." *Ibid.* Attachment A further states that the NIT will "obtain[ ] information . . . from the activating computers," which are defined as "those of any user or administrator who logs into [Playpen] by entering a username and password." *Ibid.* Henderson incorrectly states that the search warrant "erroneously described the place

to be searched as the server, located in Virginia." MTS at 17. The NIT warrant clearly states that both the server AND the computers of Playpen users who log into the website are to be searched.

The NIT warrant also describes the persons or things to be seized with particularity. The NIT warrant directs that the property to be searched is provided in Attachment B to the warrant. *See* Gov. Ex. A at 2. Attachment B, entitled the "Information to be Seized," imposed precise limits on what information could be obtained from the activating computers by the NIT. *Id.* at 4. Attachment B authorized only the seizure of the following information from any activating computer:

1) the computer's actual IP address and the date and time that the NIT determines what that IP address is;

2) a unique identifier generated by the NIT to distinguish data from that of other activating computers;

3) the type of operating system running on the computer;

4) information about whether the NIT has already been delivered to the activating computer;

5) the computer's Host Name;

6) the computer's active operating system username; and

7) the computer's media access control ("MAC") address.

Ibid.

The particularly of the place to be searched and the property to be seized pursuant to the NIT warrant is bolstered by the warrant application. The affidavit submitted with the application makes clear that "the NIT will only reveal to the government the following items, which are also described in Attachment B" and then proceeds to list the same seven items listed in Attachment B. Gov. Ex. A at 29-30, ¶ 34. A later section of the affidavit entitled "Search Authorization Requests," explains that the NIT "may cause an activating computer – *wherever located* – to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, its location, and other information about the computer and the user of the computer, as described above and in Attachment B." Gov. Ex. A at 33-34, ¶ 46(a) (emphasis added).

Henderson argues that the government failed to comply with the Fourth Amendment's particularity requirements, and "[h]ad the government particularly described the place to be searched,

i.e., a computer in San Mateo, California, no warrant could have issued." MTS 16-17. This is simply incorrect. As every court that has examined the particularity of the NIT warrant has held, the warrant did describe the place to be searched with particularity, in full compliance with the Fourth Amendment. *Michaud*, 2016 WL 337263, *5; *Stamper*, 2016 WL 695660, *19; *Epich*, 2016 WL 953269, *2; *Matish*, Dkt. 90, *32; *Darby*, 2016 WL 3189703, *8. If the government had had more particular information available at the time the warrant was issued, and had sought a warrant to search a computer in San Mateo, the Fourth Amendment's particularly requirement would not have barred such a warrant.

B. The NIT warrant complied with Rule 41, which is to be interpreted flexibly.

Henderson's argument that the NIT warrant was defective under Rule 41 of the Federal Rules of Criminal Procedure fails. The NIT warrant was consistent with Rule 41, which is to be interpreted flexibly.

At the outset, it is important to make clear the ramifications of the defendant's Rule 41 argument. At the time the government sought the NIT warrant, the defendant and thousands of others were using Playpen to share child pornography. The site was designed to hide the identity and location of its users, so the government had no way to know where the defendant was without first using the NIT authorized by the warrant. Thus, the defendant is not arguing that the government should have sought its warrant elsewhere, or that the government should have more scrupulously followed any of the procedures of Rule 41 for obtaining or executing the warrant. Instead, the defendant is arguing that his use of the Tor hidden service deprived *any* court of jurisdiction to issue a warrant to identify him. If the defendant were correct, use of a Tor hidden service could potentially create an insurmountable legal barrier to protecting the children who are harmed by massive criminal enterprises like the targeted hidden service.

1. Rule 41 is to be read broadly and interpreted flexibly.

Courts have long read Rule 41 broadly, interpreting it to permit searches where they are consistent with the Fourth Amendment even if not explicitly authorized by the text of the rule. In *United States v. New York Telephone Co.*, 434 U.S. 159 (1977), for example, the Supreme Court upheld a 20-day search warrant for a pen register to collect dialed telephone number information, despite the fact that Rule 41's definition of "property" at that time did not include information and that Rule 41 required that a search be conducted within 10 days. 434 U.S. at 169 & n.16. The Court explained that

Rule 41 "is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause," and noted that this flexible reading was bolstered by Rule 57(b), which provides, "[i]f no procedure is specifically prescribed by rule, the court may proceed in any lawful manner not inconsistent with these rules or with any applicable statute." *Id.* at 169-70.[6] Similarly, in *United States v. Koyomejian*, 970 F.2d 536 (9th Cir. 1992), the Ninth Circuit interpreted Rule 41 broadly to allow prospective warrants for video surveillance, despite the absence of provisions in Rule 41 explicitly authorizing or governing such warrants. 970 F.2d at 542.

2. The NIT warrant complied with Rule 41.

The NIT warrant is consistent with Rule 41. Rule 41(b) sets out the authority of magistrate judges to issue warrants, and three separate provisions of Rule 41(b) permitted the issuance of the NIT warrant to investigate users of Tor hidden services: Rule 41(b)(1), (2), and (4).[7]

As two district court judges have held, the NIT warrant was properly authorized as a "tracking device" pursuant to Rule 41(b)(4). *Darby*, 2016 WL 3189703, *12; *Matish*, Dkt. 90, at *39. Rule 41(b)(4) specifies that a warrant for a tracking device "may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both," provided that the tracking device is installed within the district. A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." Rule 41(a)(2)(E); 18 U.S.C. § 3117(b). This is analogous to what the NIT warrant authorized. Users of Playpen made a virtual trip via the Internet to the Eastern District of Virginia when they logged into the website with their username and password. More precisely, the Playpen users, of unknown locations, all reached into Eastern District of Virginia to access and obtain illegal child pornography. Not unlike a drug dealer who may enter another district surreptitiously and use fake identification while in the district to conceal his

---

[6] Rule 57(b) now provides: "A judge may regulate practice in any manner consistent with federal law, these rules, and the local rules of the district."

[7] In order to eliminate any ambiguity on this issue, the Supreme Court has adopted an amendment to Rule 41 to clarify that courts have venue to issue a warrant "to use remote access to search electronic storage media" within or outside an issuing district if "the district where the media or information is located has been concealed through technological means." *See* Rules of Criminal Procedure Transmittal to Congress, April 28, 2016 (available at http://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf). The new rule will take effect on December 1, 2016, unless otherwise provided by law. *See id.* at 3; *see also* 18 U.S.C. § 2074.

identity while acquiring controlled substances, the Playpen users used technology to mask their identifies when they reached into the Eastern District of Virginia to acquire child pornography. When the users logged in, the NIT was deployed onto their individual computers, which had virtually entered the Eastern District of Virginia. Then their individual computers, which may have been located outside of the Eastern District of Virginia, sent a narrow, specific set of information back to law enforcement officials. Although this network information was not itself location information, the warrant application made clear that the information sent back to law enforcement officials by the NIT would be used to try to determine the "actual location and identify" of Playpen's users. Gov. Ex. A at 27, ¶ 31; *see also id.* at 24, ¶ 32 (explaining that "using a NIT may help FBI agents locate the administrators and users" of Playpen); *id.* at 25, ¶ 34 (stating that the NIT will reveal information "that may assist in identifying the user's computer, its location, and the user of the computer"); *id.* at 26, ¶ 35 (same).

The Eastern District of Virginia magistrate judge also had authority under Rule 41(b)(2) to issue the NIT warrant. Rule 41(b)(2) allows a magistrate judge "to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." Here, the warrant authorized use of the NIT on a server in the Eastern District of Virginia. Gov. Ex. A at 22-24, ¶¶ 30, 33. The NIT was deployed only to registered users of Playpen who logged into the website, which was located on a server in the Eastern District of Virginia, with a username and password. *Id.* at 3. Each of these users and their individual computers—including Henderson and his computer—virtually reached into the Eastern District of Virginia to access the Playpen website. The property seized, that is, the information that the NIT directed each user's computer to send to law enforcement officials, virtually resided in the Eastern District of Virginia. *See* Fed. R. Crim. P. 41(a)(2)(A) (defining "property" to include both "tangible objects" and "information"). Thus, Rule 41(b)(2) provided sufficient authority to issue the warrant for use of the NIT outside of the Eastern District of Virginia.

Finally, the NIT warrant was issued by a judge in the district with the strongest known connection to the search. Henderson entered the Eastern District of Virginia by accessing the Playpen website, which resided on a server in that District; he retrieved the NIT from that server; and the NIT sent his network information back to a computer in that District. The magistrate judge had authority

under Rule 41(b)(1) to authorize a search warrant for "property located within the district." The use of the Tor hidden service by Henderson and other Playpen users made it impossible for investigators to know in what other districts, if any, the execution of the warrant would take place. Under these circumstances, it was reasonable for the Eastern District of Virginia magistrate judge to issue the warrant. Interpreting Rule 41 to allow the issuance of warrants like the NIT warrant does not risk significant abuse because, as with all warrants, the manner of execution "is subject to later judicial review as to its reasonableness." *Dalia v. United States*, 441 U.S. 238, 258 (1979). For these reasons, this Court should conclude that issuance of the warrant did not violate Rule 41.

Henderson cites a single magistrate judge's opinion holding that Rule 41(b) does not authorize issuance of a warrant for use of a different (and significantly more invasive) NIT than the one used in this case. MTS, at 13 (*citing In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013)). *In Re Warrant*, though, does not undermine the magistrate judge's decision to issue the NIT warrant. The decision of one magistrate judge in one district about a different NIT could be of persuasive value, but the decision of the issuing magistrate in this case is significantly more pertinent. First, *In re Warrant* appears to be an outlier. To the government's knowledge, in every other matter involving an application for a search warrant to identify a person hiding his identity and location using Internet anonymizing techniques, the judge has issued the warrant. *See, e.g., United States v. Cottom, et. al.*, No. 13-cr-108 (D. Neb. Oct. 14, 2014) (Doc #122, Attachment 1; Doc. #123, Attachment 1) (2 separate NIT search warrants), (Doc #155) (denying suppression motion); *United States v. Welch*, 811 F.3d 275 (8th Cir. 2016) (affirming denial of suppression motion in related case); *In re Search of NIT for Email Address texas.slayer@yahoo.com*, No. 12-sw-5685 (D. Col. October 9, 2012) (Doc #1) (search warrants); *In re Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to That Account by the Government*, No. 07-mj-5114 (W.D. Wash. June 12, 2007), available at http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf.

Moreover, the reasoning of the Texas magistrate judge's decision does not apply to the use of the NIT in this case. That court correctly found it "plausible" that the NIT fell within the definition of a tracking device. 958 F. Supp. 2d at 758. Nevertheless, the court held that Rule 41(b)(4) did not apply

because there was no showing that the installation of the NIT software would be within its district. *See ibid.* That was not the case here: installation of the NIT within the meaning of Rule 41(b)(4) took place on the server in the Eastern District of Virginia. As the analogy to physical tracking devices demonstrates, the government "installed" the NIT within the meaning of Rule 41(b)(4) when it added the NIT to the computer code on the Playpen website, which resided in the Eastern District of Virginia. Henderson's subsequent retrieval of the NIT and its collection of information from his computer constituted "use of the device" for purposes of Rule 41(b)(4), regardless of whether that process of collection included "installation" on Henderson's computer.

C. The NIT warrant was justified based on exigent circumstances.

Even if the NIT warrant somehow ran afoul of Rule 41, its use would be justified based on exigent circumstances. The Supreme Court has recognized that the presumption that warrantless searches are unreasonable "may be overcome in some circumstances because '[t]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011). "One well-recognized exception applies when the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment." *Id.* (internal quotation marks omitted). The Ninth Circuit has defined exigent circumstances as "those circumstances that would cause a reasonable person to believe that entry . . . was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." *United States v. Martinez*, 406 F.3d 1160, 1164 (9th Cir. 2005) (quoting *United States v. McConney*, 728 F.2d 1195, 1199 (9th Cir.1984) (*en banc*) (abrogated on other grounds)). Courts must evaluate "the totality of the circumstances" to determine whether exigencies justified a warrantless search. *Missouri v. McNeely*, 133 S. Ct. 1552, 59 (2013).

Here, even if the government could not have obtained the NIT warrant under a restricted reading of Rule 41(b), ample exigent circumstances existed to justify the use of the NIT. Playpen enabled ongoing sexual abuse and exploitation of children, and deploying the NIT against Playpen users was necessary to stop the abuse and exploitation, uncover hidden evidence and identify and apprehend the abusers. Since the NIT was used to identify and locate users of Playpen, the FBI has been able to

identify or recover child victims from abuse, and has also identified "hands on" child sexual offenders and child pornography producers.

The information the NIT collected was also fleeting. If law enforcement had not collected IP address information at the time of user communications with Playpen, then, due to the site's use of Tor, law enforcement would have been unable to collect identifying information. Accordingly, if the warrant could not have been issued, then no warrant could have been obtained in a reasonable amount of time to identify perpetrators. *See United States v. Struckman*, 603 F.3d 731, 738 (9th Cir. 2010) (stating that to invoke the exigent circumstances exception, "the government must . . . show that a warrant could not have been obtained in time").

Moreover, the NIT warrant was minimally invasive and specifically targeted at the fleeting identifying information: it only authorized collection of IP address information and other basic identifiers for site users. And Playpen's users, including the defendant, lacked a reasonable expectation of privacy in their IP addresses. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007) (holding that a defendant lacks a reasonable expectation of privacy in IP addresses). The defendant's use of Tor does not alter this premise, as the defendant still had to convey his IP address to a third party to access the Tor nodes. Nor does the defendant claim that he had a reasonable expectation of privacy in any of the information retrieved by the NIT. Additionally, multiple courts that have examined the NIT warrant have held that the defendants had no reasonable expectation of privacy in their IP addresses. *See Matish*, Dkt. 90, at *46; *Werdene*, 2016 WL 3002376, *17-18; *Stamper*, 2016 WL 695660, *21–22; *Michaud*, 2016 WL 337263, *14. Therefore, even if no court had authority to issue a warrant to deploy a NIT to investigate Playpen users in Washington, as Henderson essentially argues is the case, its use was nonetheless reasonable under the Fourth Amendment.

D. The NIT warrant complied with 28 U.S.C. § 636(a).

In a passing and conclusory fashion, the defendant also cites 28 U.S.C. § 636(a) as a separate ground in support of his motion to suppress. 28 U.S.C. § 636(a) provides that magistrate judges shall have within their district and "elsewhere as authorized by law . . . all powers and duties conferred or imposed upon the United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts." The defendant spends little or no time distinguishing Rule 41 from 28

U.S.C. § 636(a). The same rationale for determining that the NIT warrant complied with Rule 41 applies to section 636(a): the NIT warrant was authorized by Rule 41, and therefore, the magistrate judge was, by definition, acting within the powers prescribed by section 636(a).

E. Even assuming arguendo that the NIT warrant was lacking, suppression is not an appropriate remedy.

Assuming arguendo that the warrant was somehow deficient under Rule 41, suppression is neither required by law nor reasonable under the circumstances. "Rule 41 violations fall into two categories: fundamental errors and mere technical errors." *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992). "Fundamental errors are those that result in clear constitutional violations." *Id.* By contrast, technical errors may only trigger suppression upon a proper showing of prejudice or "deliberate disregard" for Rule 41. *Id.*

Suppression is a "last resort, not [the courts'] first impulse," and any benefit to doing so (general deterrence of law enforcement misconduct) must outweigh the substantial social cost that results when "guilty and possibly dangerous defendants go free." *Herring v. United States*, 555 U.S. 135, 140-41 (2009). Accordingly, defendants who seek suppression must clear a "high obstacle," *id.* at 141, and "resolution of doubtful or marginal cases . . . should largely be determined by the preference to be accorded to warrants." *United States v. Kelley*, 482 F.3d 1047, 1050-51 (9th Cir. 2007) (citing and quoting *Illinois v. Gates*, 462 U.S. 213, 237 n.10 (1983)).

In the Rule 41 context in particular, the Ninth Circuit has observed, "we have repeatedly held—and have been instructed by the Supreme Court—that suppression is rarely the proper remedy for a Rule 41 violation." *United States v. Williamson*, 439 F.3d 1125, 1132 (9th Cir. 2006). "Because the exclusionary rule tends to exclude evidence of high reliability, the suppression sanction should only be applied when necessary and not in any automatic manner." *United States v. Luk*, 859 F.2d 667, 671 (9th Cir. 1988) (affirming denial of suppression motion despite a technical violation of Rule 41). Whether exclusion is warranted "must be evaluated realistically and pragmatically on a case-by-case basis." *Id.* (quoting *United States v. Vasser*, 648 F.2d 507, 510 n.2 (9th Cir. 1981)).

None of the three bases that Henderson alleges warrant suppression withstand scrutiny.

1. The magistrate judge did not lack statutory authority to issue the NIT warrant.

The magistrate judge was authorized pursuant to Rule 41(b) and 28 U.S.C. § 636(a) to issue the NIT warrant to search for activating computers, wherever located, that accessed Playpen to view, download, and distribute child pornography. Even assuming arguendo that section 636(a) and Rule 41(b) did not permit the magistrate judge to issue a warrant for the search of activating computers that were located in other districts, Henderson's argument that the magistrate judge was wholly without authority to approve the NIT warrant is erroneous. *See* MTS, at 14-15. Rule 41(b) permitted the magistrate judge, at a minimum, to issue the NIT warrant for the search of activating computers located within the Eastern District of Virginia and within the territorial and diplomatic areas listed in subsection (5). Since the magistrate judge acted well within her authority to approve the search warrant for these locations, it cannot be said that "[t]he magistrate judge was never authorized to issue the NIT warrant." *MTS*, at 15.

That the NIT warrant could have been and in fact was validly executed in the Eastern District of Virginia, *see, e.g., Darby*, 2016 WL 3189703; *Matish*, Dkt. 90, distinguishes this case from *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), and *United States v. Glover*, 736 F.3d 509 (D.C. Cir. 2013), which the defendant relies upon to argue that the NIT warrant is no warrant at all. In both *Krueger* and *Glover*, the warrant applications presented to the judge for approval made clear that the place to be searched was not within the authorizing judge's district. *Krueger*, 809 F.3d at 1111 (warrant presented to magistrate judge in the District of Kansas asked for permission to search home and vehicle located in Oklahoma); *Glover*, 736 F.3d at 510 (warrant presented to district court judge in the District of Columbia asked for permission to install tracking device on vehicle located in Maryland). As a consequence, the respective courts of appeal concluded that the warrants were invalid at the time they were issued because the territorial limitations of Rule 41 (and in *Glover*, of Title III) did not authorize the judges to issue warrants for searches in other districts. *Krueger*, 809 F.3d at 1116-17, 1118 (Gorsuch, J., concurring); *Glover*, 736 F.3d at 515. Here, in contrast, the NIT warrant application presented to the magistrate judge asked for permission to search the "activating computers—wherever located" that accessed the Playpen server located in the Eastern District of Virginia. Unlike the warrants

in *Krueger* and *Glover*, the NIT warrant did not specify that the search would occur only outside of the Eastern District of Virginia, and since the warrant also contemplated a search within the authorizing judge's district, it was presumptively valid at the time it was issued.

2. Henderson has failed to show that he was prejudiced.

Henderson wrongly argues that he suffered such prejudice that suppression is necessary. MTS, at 15-17. However, any deviation from the letter of Rule 41 was the product of Playpen's users (including Henderson) using Tor to evade law enforcement, not some bad faith on the part of law enforcement in trying to comply with Rule 41. The Ninth Circuit has found no prejudice to exist from a Rule 41 violation where "the circumstances under which the warrant was sought at least partially justified the agents' deviation from the letter of the Rule" and the warrant "complies with the spirit of Rule 41 in that it provided a basis for a probable cause determination and established an adequate record to review that determination." *United States v. Vassar*, 648 F.2d 507, 510 (9th Cir. 1980). Even if the NIT warrant ran counter to the letter of Rule 41, it certainly still complied with Rule 41 in spirit. *See Michaud*, 2016 WL 337263, *6.

Henderson claims that no magistrate judge would have had the authority to issue the NIT warrant, and that without the NIT warrant, law enforcement officials would not have been able to obtain the San Mateo warrant. MTS. 15-16. He essentially argues that the first search would not have occurred if Rule 41(b) had been followed, and therefore, he suffered prejudice. This would mean that any violation of Rule 41(b), no matter how small, would constitute sufficient prejudice to warrant suppression. The Ninth Circuit specifically rejected that argument in *Vassar*, 648 F.2d at 510 n.2, as has one district court that examined the NIT warrant. *See Michaud*, 2016 WL 337263, *6-7.

At its core, Henderson's argument is that no court anywhere could have issued a warrant to permit a search of his computer because the server hosting Playpen was situated in a different district and he used Tor to hide his location. That is not the sort of claimed "prejudice" that should result in suppression. Having already used Tor to shield his location from investigators, under no reasonable analysis should Henderson be permitted to wield it as a sword to defeat the government's ability to obtain judicial authorization to search for the true location from which he accessed child pornography. "The policies behind the exclusionary rule are not absolute and must be evaluated realistically and

pragmatically on a case by case basis." *Vassar*, 648 F.2d at 510 n.2. Nor should this court "fault the good faith ingenuity of the officers" in responding to the defendant's use of advanced technology with its own, where "interests protected by the fourth amendment and Rule 41 were safeguarded by the officers . . . even though the methods used were novel." *Id.*

Indeed, had Henderson not concealed his true location, the government could have obtained a search warrant from a magistrate judge in this district. *See United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005) (rejecting claim of prejudice where law enforcement officer could have obtained warrant from a separate judicial officer); *United States v. Johnson*, 660 F.2d 749, 753 (9th Cir. 1981) (same). In any event, as noted above, the government nonetheless could have proceeded with the NIT search without a warrant, due to the exigent circumstances created by Henderson's use of the Tor network to conceal his location and identity.

3. Law enforcement acted in good faith and did not deliberately disregard Rule 41.

Suppression is also unwarranted because the government acted in good faith and did not intentionally and deliberately disregard Rule 41(b). In the Ninth Circuit, suppression is only warranted in the case of a deliberate violation of Rule 41 if that violation occurs in "bad faith." *See Luk*, 859 F.2d at 673 ("suppression is required for nonfundamental violations in bad faith"); *see also Williamson*, 439 F.3d at 1134 ("Other cases have equated 'deliberate and intentional disregard' with 'bad faith.'"). The good faith exception also bars suppression even if the Court determines that the NIT warrant did not comply with the Fourth Amendment. Under the good faith exception to the Fourth Amendment's exclusionary rule, suppression is not warranted where officers rely in good faith on an objectively reasonable search warrant issued by a neutral and detached judge. *United States v. Leon*, 468 U.S. 897, 900 (1984). This objective standard is measured by "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Id.* at 922 n.23. "[A] warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *Id.* at 922 (quotation marks omitted). The Supreme Court observed that "suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of

exclusionary rule." *Id.* at 918. The Court identified only four circumstances where exclusion is appropriate: where (1) the issuing magistrate was misled by the inclusion of knowing or recklessly false information; (2) the issuing magistrate wholly abandoned the detached and neutral judicial role; (3) the warrant is facially deficient as to its description of the place to be searched or the things to be seized; or (4) the affidavit upon which the warrant is based is so lacking in indicia of probable cause that no reasonable officer could rely upon it in good faith. *Id.* at 923-24. None apply here. Indeed, defendant fails to even argue that any of these factors are present.

Here, the warrant affidavit contained no knowingly or recklessly false information that was material to the issue of probable cause. Nor does Henderson allege that the issuing magistrate abandoned her judicial role. The warrant clearly and particularly described the locations to be searched and the items to be seized. And the affidavit made a strong, comprehensive showing of probable cause to deploy the NIT. Absent any of these errors, once the magistrate judge signed the warrant after having been made aware of how the NIT would be implemented and its reach, the agents' reliance on that authority was objectively reasonable. *See Massachusetts v. Sheppard*, 468 U.S. 981, 989-90 (1984) ("[W]e refuse to rule that an officer is required to disbelieve a judge who has just advised him, by word and by action, that the warrant he possesses authorizes him to conduct the search he has requested").

The same holds true for any alleged Rule 41 infirmity. *See Negrete-Gonzales*, 966 F.2d at 1283 (applying good faith doctrine in the context of a Rule 41 violation). "The Supreme Court's goal in establishing the good-faith exception was to limit the exclusionary rule to situations where the illegal behavior of officers might be deterred." *United States v. Gantt*, 194 F.3d 987, 1006 (9th Cir. 1999).

The actions at issue here hardly come close to constituting "illegal behavior" or "police misconduct," *id.*, warranting the extreme remedy of suppression. First, law enforcement officials sought a warrant from a neutral and detached judge to deploy the NIT, which the Ninth Circuit recognizes as "the most fundamental policy of the Rule." *Luk*, 859 F.2d at 674. Moreover, law enforcement supported its request with a 31-page affidavit that explained in detail the abundant probable cause justifying the deployment of the NIT, the location-obscuring technology Henderson and others used to evade law enforcement and disseminate child pornography, the fact that the NIT would reach computers wherever they might be, and the limited pieces of information the NIT would retrieve. Further, law

enforcement sought this authorization from the district where Playpen would operate and in which Henderson and others would enter to access the site. To the extent no other district was available, that was purely due to the purposeful use of sophisticated technology by Henderson and others to mask their true location. Accordingly, any jurisdictional flaw under Rule 41 was the product of a good faith effort to identify an appropriate venue, consistent with Rule 41, from which to seek a warrant, not an effort to circumvent the Rule's requirements. Under these circumstances, the officers' reliance on the warrant was objectively reasonable, regardless of any flaws it may have had, and the good faith exception precludes suppression. *Gantt*, 194 F.3d at 1005 ("If the executing officers act in good faith and in reasonable reliance upon a search warrant, evidence which is seized under a facially valid warrant which is later held invalid may be admissible." (quotation marks omitted)); *see also Sheppard*, 468 U.S. at 987-88. Ultimately, agents acted reasonably in relying upon the magistrate's authorization of the NIT warrant, and so the evidence seized pursuant to it should not be suppressed.

Henderson nonetheless insists that the government committed an intentional violation of Rule 41, pointing to the government's proposal and support of an amendment to Rule 41. *See* MTS, at 18. The proposed amendment to Rule 41 was intended to clarify that courts have venue to issue a warrant "to use remote access to search electronic storage media" inside or outside an issuing district if "the district where the media or information is located has been concealed through technological means." This proposed amendment and the accompanying letter from the then-Assistant Attorney General for the Criminal Division of the Department of Justice prove the government recognized the need for clarification. They do not reflect a concession that but for that clarification, Rule 41 is a bar to the approach taken by the government in this case. That the Department of Justice seeks greater clarity in the Rule does not convert conduct taken in good faith to a deliberate and intentional violation of the rule. Moreover, at the time the Department of Justice proposed the Rule 41 Amendment, a single magistrate judge in one case had rejected a warrant to locate a computer concealed through technological means, but every other magistrate judge known to consider the issue had issued such a warrant.

IV. CONCLUSION

For all the foregoing reasons, the Court should deny the defendant's motion to suppress evidence.

DATED this 1st day of July, 2016.

Respectfully submitted,

BRIAN J. STRETCH
United States Attorney

HELEN L. GILBERT
Assistant United States Attorney